Date of Hearing: March 18, 2025
Fiscal: No

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 446 (Ward) – As Introduced February 6, 2025

PROPOSED AMENDMENTS

SUBJECT: Surveillance pricing

SYNOPSIS

AB 375 (Chau, Ch. 55, Stats. 2018), the California Consumer Privacy Act, established a framework for transparency regarding consumer data collection. In 2020, voters expanded these protections by passing Proposition 24, which created the California Privacy Protection Agency and strengthened consumer data rights. Despite these efforts, businesses continue to collect vast amounts of personally identifiable information to develop personalized experiences, sometimes to the detriment of consumers.

Over the past decade, consumer rights groups have documented instances of real-time price changes based on consumer data. These examples have raised concerns about businesses' ability to analyze a consumer's willingness to pay and adjust prices accordingly without consumer knowledge or consent.

This bill, sponsored by Consumer Watchdog and United Food and Commercial Workers Western States Council, would impose a blanket ban on personalized price discrimination – "surveillance pricing" – based in whole or in part on the consumer's personally identifying information. The bill provides consumers with recourse against businesses that violate this prohibition.

The bill is supported by numerous consumer rights and labor organizations, including the California Nurses Association, Oakland Privacy, and California Federation of Labor Unions. The bill is opposed by a variety of business trade associations, including the California Chamber of Commerce and the American Advertising Federation.

Some of their principal concerns are addressed in Committee amendments, set forth in Comment 5, which refine the bill's scope, exempting common pricing practices such as differences of cost of business, loyalty programs, and discounts for specific groups, such as teachers, active service members, and senior citizens. Committee amendments also clarify definitions of personally identifiable information, exempt insurers, and remove the bill's findings and declarations.

If passed by this Committee, the bill will next be heard by Assembly Judiciary Committee.

THIS BILL:

1) Prohibits a person from engaging in surveillance pricing.

2) Defines "surveillance pricing" as when a person sets a price offered to a consumer based, in whole or in part, upon personally identifiable information gathered through an electronic surveillance technology, including electronic shelving labels.

3) Defines "electronic surveillance technology" as a technological method or system of surveillance used to observe, monitor, or collect information related to a person and includes any of the following information about the person:

    a. Actions, habits, race, religion, residence, sexuality, or preferences.

    b. Interests, including the individual's political, personal, or professional affiliation.

    c. Web browsing history, purchase history, financial circumstances, or consumer behaviors.

    d. Personally identifiable information.

4) Incorporates the definition of "personally identifiable information" from the California Consumer Privacy Act (CCPA) and also provides that, for purposes of the bill, this term includes deidentified or aggregated consumer information.

5) Subjects violators to a civil penalty for violations, treble damages and disgorgement of revenues earned for intentional violations, and reasonable attorney's fees and costs.

6) Provides that waivers of the bill are against public policy and are void and unenforceable.

EXISTING LAW:

1) Provides that, among other rights, all people have an inalienable right to pursue and obtain privacy. (Cal. Const., art.1, § 1.)

2) Establishes the Unruh Civil Rights Act. (Civil Code § 51.)

3) Establishes the CCPA, which grants consumers certain rights with regard to their personal information, including enhanced notice, access, and disclosure; the right to deletion; the right to restrict the sale of information; and protection from discrimination for exercising these rights. Places attendant obligations on businesses to respect those rights. (Civ. Code § 1798.100 et seq.)

4) Establishes the California Privacy Protection Agency (Privacy Agency) and vests it with full administrative power, authority, and jurisdiction to implement and enforce the CCPA. (Civ. Code § 1798.199.10.)

5) Establishes the Unfair Practices Act (UPA), which is intended to safeguard the public against the creation or perpetuation of monopolies and to foster and encourage competition, by prohibiting unfair, dishonest, deceptive, destructive, fraudulent and discriminatory practices by which fair and honest competition is destroyed or prevented. (Bus. & Prof. Code § 17000 et seq.)

6) Prohibits, under the UPA, a range of behavior that reduces competition in pricing, including specified locality discrimination in pricing, sales under costs or loss leaders made with the intent of injuring competitors or destroying competition, and contracts for the performance of warranty service and repair below the cost of the service or repair. (Bus. & Prof. Code, §§ 17040-17051.)

7) For purposes of investigating potential violations of the UPA, extends all of the investigative powers granted to the Attorney General pursuant to 7) to the district attorney of any county when the district attorney reasonably believes that a violation has occurred. (Bus. & Prof. Code § 16759(a).)

COMMENTS:

1) **Author's statement**. According to the author:

> With the rise of artificial intelligence and data collection, businesses increasingly use personal data to set prices, often leading to unfair and discriminatory pricing practices. This legislation aims to establish safeguards that ensure transparency, fairness, and consumer protections in pricing algorithms. AB 446 will prohibit the practice of surveillance pricing by making it unlawful for businesses to use personal data when charging different prices for the same product, or service whether online or during in-store checkout.

2) **The Commodification of Personal Data**. Enshrined in the state constitution by a ballot initiative in 1972, the unalienable right to privacy is guaranteed to all Californians and is enforceable against both the public and private sectors. However, for the past 20 years, experts have been warning us about the erosion of our private lives. They note that this erosion is happening one small bit at a time, likely without people even noticing. With the advent of the internet and advances in technology, it is no longer easy for people to decide which aspects of their lives should be publicly disclosed. As Alex Preston noted in *The Guardian* a decade ago:

> We have come to the end of privacy; our private lives, as our grandparents would have recognised them, have been winnowed away to the realm of the shameful and secret. . . . Insidiously, through small concessions that only mounted up over time, we have signed away rights and privileges that other generations fought for, undermining the very cornerstones of our personalities in the process. While outposts of civilisation fight pyrrhic battles, unplugging themselves from the web. . . the rest of us have come to accept that the majority of our social, financial and even sexual interactions take place over the internet and that someone, somewhere, whether state, press or corporation, is watching.[1]

Since this piece was published, it has become increasingly clear that not only is our right to privacy significantly eroded, but our private information and activities are now being harvested and sold for a profit. This commodification of personal information has been dubbed "surveillance capitalism" by social psychologist, Shoshana Zuboff. In an opinion piece for *The New York Times*, in 2021, Dr. Zuboff warned:

> As we move into the third decade of the 21st century, surveillance capitalism is the dominant economic institution of our time. In the absence of countervailing law, this system successfully mediates nearly every aspect of human engagement with digital information. The promise of the surveillance dividend now draws surveillance economics into the "normal" economy, from insurance, retail, banking and finance to agriculture, automobiles, education, health care and more. . . .

---

[1] Preston, Alex. "The death of privacy." *The Guardian* (Aug. 3, 2014), https://www.theguardian.com/world/2014/aug/03/internet-death-privacy-google-facebook-alex-preston.

> An economic order founded on the secret massive-scale extraction of human data assumes the destruction of privacy as a nonnegotiable condition of its business operations. With privacy out of the way, ill-gotten human data are concentrated within private corporations, where they are claimed as corporate assets to be deployed at will.[2]

The rapid advancement of artificial intelligence over the past five years has significantly accelerated data collection and processing. AI agents can be deployed to extract data, also known as scraping, from websites. Inevitably this includes personal information of consumers which data brokers compile and sell to businesses. These businesses then integrate the acquired data with their own consumer information to create detailed consumer profiles. With AI, these profiles can be updated in real time to personalize user experiences and target advertisements more effectively.

3) **Background**. For much of history, deals at marketplaces were made via bartering, and consumers and producers alike would try to haggle a deal that would align with the buyer's willingness, or ability, to pay for a good. This system enabled some consumers to cut deals; however, others would be taken advantage of because of the lack of transparency in how much a product actually cost. The bartering system was upended in mid 1800s when a Wanamaker's department store in Philadelphia began to include price tags on their goods. John Wanamaker believed that customers would trust their retailers more if they could see the prices and, therefore, make informed decisions about their purchasing options.[3] He incorporated these prices into advertisements, and when customers found them to be accurate, it strengthened their confidence in the retailer. This innovation helped drive the expansion of department stores and set the standard for pricing practices for the next 150 years.

Surveillance pricing, also known as individualized pricing, uses AI or other technology for the real-time processing of personal information about a consumer to set a price specific to that consumer. The Federal Trade Commission (FTC) has described surveillance pricing as "an ecosystem designed to use large-scale data collection to help sellers maximize their revenues by customizing the pricing, as well as the selection of products and services, offered to each consumer."[4]

It is important to distinguish surveillance pricing from dynamic pricing, which adjusts prices in response to market demand. For example, Ticketmaster uses dynamic pricing to increase ticket prices for all consumers when demand rises.[5] In contrast, surveillance pricing treats each consumer as their own economy, using algorithms to assess their willingness to pay based on personal information such as browsing history, purchase behavior, and location.

---

[2] Zuboff, Shoshana. "You Are the Object of a Secret Extraction Operation." *The New York Times* (Nov. 12, 2021) *available at* https://www.nytimes.com/2021/11/12/opinion/facebook-privacy.html.
[3] PBS, "John Wanamaker" (Mar. 10, 2025), https://www.pbs.org/wgbh/theymadeamerica/whomade/wanamaker_hi.html.
[4] Federal Trade Commission, "Issue Spotlight: The Rise of Surveillance Pricing" (January 17, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer.
[5] Cody Mello-Klein, "What is dynamic pricing and why is it hiking ticket prices for Oasis, Taylor Swift and your favorite artist?", *Northeastern Global News* (Oct. 2, 2024), https://news.northeastern.edu/2024/10/02/dynamic-pricing-ticketmaster-oasis-taylor-swift/.

Surveillance Pricing has already impacted consumers. In 2012, *The Wall Street Journal* reported that the retailer Staples used an algorithm that set higher prices for consumers who lived further from a rival store.[6] Target also used an algorithm to adjust the price of a TV once a customer entered the parking lot, leading to a $5 million settlement with the City of San Diego for false advertising and unfair business practices related to surveillance pricing.[7] The *SF Gate* recently reported that Bay Area consumers are offered a higher price than users in either Phoenix or Kansas City for the same exact hotel reservations on various hotel booking websites.[8] California Chamber of Commerce, along with multiple trade organizations, argues that these differences in pricing are a result of California laws regarding transparency:

> This discrepancy is because California law recently changed to require all included fees for any hotel rooms to be included in the up-front price. AB 537 (Berman) compelled online travel sites to list their prices including all fees up front – and Cal Chamber (along with other opposition groups) repeatedly testified that such a process would confuse consumers by making it appear that prices were actually different for California consumers and out-of-state consumers. Now, it appears consumer groups are indeed confused and are alleging that businesses' appropriate compliance with recent law is actually something nefarious.

While it is likely that some differences in prices could be due to the compelled fee disclosures, the difference per night for an SF resident compared to a Phoenix resident at the same hotel for the same booking was $511 higher – which simply cannot be due solely to discrepancies from transparency. This is appears to have been tacitly acknowledged by Booking in its response to this investigation:

> In an email, Angela Cavis, spokesperson for Booking, said that the rates users see were "determined by our accommodation partners, who have full control over the rates they choose to list on the site." Cavis explained that, "Partners also have the flexibility to create specific promotional rates, such as country rates or mobile rates, which are designed to offer discounts, not charge higher prices."[9]

Moreover, the use of AI to set prices raises concerns regarding biases within the algorithms that may disadvantage different groups. A 2021 study from George Washington University found that Uber and Lyft charged, on average, higher prices for pickups and drop-offs in predominantly non-white neighborhoods or neighborhoods with lower incomes.[10] While it is unclear whether these disparities stem from market forces or algorithmic bias because these companies use opaque algorithms to set prices, a possible conclusion is that algorithmic price setting could reinforce structural inequities.

---

[6] Jennifer Valentino-DeVries, Jeremy Singer-Vine and Ashkan Soltani, "Websites Vary Prices, Deals Based on Users' Information," *Wall Street Journal* (Dec. 24, 2012), https://www.wsj.com/articles/SB10001424127887323777204578189391813881534.
[7] Chris Hrapsky, "Target settles lawsuit alleging false advertising, overpricing; fined $5M", *KARE* (Apr. 27, 2022), https://www.kare11.com/article/news/local/kare11-extras/target-settles-ca-lawsuit-alleging-false-advertising-overpricing-fined-5m/89-ba4a5441-c38e-4c9f-b524-b0d13414042f.
[8] Keith A. Spencer, "Hotel booking sites show higher prices to travelers from Bay Area," *SFGATE* (Feb. 3, 2025), https://www.sfgate.com/travel/article/hotel-booking-sites-overcharge-bay-area-travelers-20025145.php.
[9] *Ibid*.
[10] Akshat Pandey and Aylin Caliskan, "Disparate Impact of Artificial Intelligence Bias in Ridehailing Economy's Price Discrimination Algorithms" *arXiv* (May 3, 2021), https://arxiv.org/abs/2006.04599.

Because businesses often operate without transparency, the extent of surveillance pricing remains uncertain. In the summer of 2024, the Federal Trade Commission launched a study to investigate how companies leverage AI, other technologies, and consumer data to set individualized prices. A preliminary report released in January revealed that at least 250 businesses have adopted technologies capable of implementing surveillance pricing. Lina Khan, former FTC Chair, concludes in this report:

> "Initial staff findings show that retailers frequently use people's personal information to set targeted, tailored prices for goods and services—from a person's location and demographics, down to their mouse movements on a webpage. The FTC should continue to investigate surveillance pricing practices because Americans deserve to know how their private data is being used to set the prices they pay and whether firms are charging different people different prices for the same good or service."[11]

More efficient markets vs competition. Surveillance pricing has the potential to create more efficient markets. By accurately scaling prices to a consumer's willingness to pay, businesses can sell more goods and services to a broader customer base. Underserved populations could benefit from greater discounts, increasing their access to markets that were previously unavailable to them. In theory, this could enhance overall consumer welfare.

However, this would also suggest that someone with a high willingness to pay would be charged a higher price to offset those discounts. This raises concerns about fairness and could have a chilling effect on those high willingness consumers, making them less likely to participate in the marketplace.

Surveillance pricing is an example of perfect price discrimination. Under perfect price discrimination, consumer surplus, the difference between what a consumer is willing to pay and the actual price they pay, disappears as each consumer is charged exactly what they are willing to pay.[12] Therefore, all surplus in the market is captured by the producer, which can reduce consumer welfare. The FTC has reported on this phenomena finding that businesses that had implemented surveillance pricing had already seen 1-5% increases in revenue.[13] In contrast, traditional competitive pricing exerts downward pressure on prices, increasing consumer surplus and overall consumer welfare, though at the cost of some inefficiency, or deadweight loss, for producers.

Research suggests that surveillance pricing, under highly competitive pressures, could lead to aggressive pricing strategies taken by all firms that result in lower prices.[14] However, this outcome depends on consumer data being used solely for pricing, data is equally available, and the data is not used for other strategic purposes. In less competitive markets, or where one firm

---

[11] Federal Trade Commission, "FTC Surveillance Pricing Study Indicates Wide Range of Personal Data Used to Set Individualized Consumer Prices" (Mar. 10, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer.

[12] Organisation for Economic Co-operation and Development "Personalised Pricing in the Digital Era" (Mar. 10, 2025), https://web-archive.oecd.org/temp/2022-02-22/494784-personalised-pricing-in-the-digital-era.htm

[13] Federal Trade Commission, "FTC Surveillance Pricing 6(b) Study: Research Summaries A Staff Perspective" (Jan. 17, 2025), p. 10.

[14] Zhijun Chen, Chongwoo Choe, Noriaki Matsushima, "Competitive Personalized Pricing", *Management science*, vol. 66, No. 9, September 2020, p. 3799

has superior access to consumer data, surveillance pricing can instead be used to target specific consumers with personalized discounts, ads, and product recommendations. This strategy fosters customer loyalty, making those consumers less price-sensitive and increasing the cost for competitors to attract them. Competition then softens which leads to higher costs for consumers. Smaller firms that cannot afford to collect, purchase, or process vast consumer datasets will face increasing disadvantages if surveillance pricing becomes widespread. This imbalance could further entrench market power among large corporations, reducing competition and ultimately harming consumers.

The UCFW Western States Council summarizes:

> "A too-often overlooked aspect of functioning markets is how they permit personal autonomy and freedom. Rather than only being able to build personal wealth by working for a giant company, an individual armed with a good idea, some savings or modest capital, and grit, can in a competitive market choose to earn a living by profitably working for themselves.
>
> But, if a pre-requisite to being able to compete profitably in every market is access to the world's biggest computers, the richest repositories of personal behavioral data, and most powerful AI, such entrepreneurial individual choices and freedoms become either impossible or restrained only to tiny, Etsy-like, boutique ambitions."

Surveillance pricing raises concerns for price-setting collusion. Market-wide implementation of surveillance pricing may raise antitrust concerns due to the risk of tacit algorithmic collusion. Though many firms may create their own models for personalized price setting, others may outsource their price-setting to a third party. If these third parties use private data supplied by multiple firms, price collusion could result, raising questions of antitrust enforcement. Legislative efforts regarding algorithmic price collusion are currently underway.

Last session, SB 1154 (Hurtado, 2024) would have prohibited the use of algorithms to set or recommend prices or commercial terms that incorporate nonpublic competitor data. This bill died in Senate Judiciary. This session, there are currently three bills, AB 325 (Aguiar-Curry), SB 295 (Hurtado), and SB 384 (Wahab) seeking to prohibit the use of algorithms to set or recommend prices that incorporate nonpublic competitor data. SB 52 (Perez) similarly would prohibit the use of algorithms that incorporate nonpublic competitor data concerning local and statewide rents or occupancy levels for the purpose of setting rent prices. The prohibition of surveillance pricing would likely not impact the implementation of any of these bills focusing on algorithmic price collusion, though this serves to highlight the extent to which the legislature views algorithmic price setting as a pertinent issue.

3) **What this bill would do.** As noted above, many businesses collect, collate, and process large amounts of data about their consumers, including data about the consumer's employment, shopping habits, and browser history. Companies with access to this data can implement surveillance pricing, a practice of setting individualized prices based on a consumer's perceived willingness to pay. One argument for this practice is that real-time, personalized pricing could expand market access by allowing more consumers to purchase goods and services at prices tailored to them. Willingness to pay, though, does not necessarily correspond with ability to pay or value. A parent may be more willing to pay for cold medicine when their child is sick, but should that willingness justify higher prices? In a bartering system, the consumer at least had the

ability to negotiate for a better deal, with surveillance pricing, the consumer may not even know that the price has been adjusted.

Additionally, surveillance pricing incentivizes the continual collection of consumer data, raising privacy concerns, and gives advantages to larger firms with access to more information and better technology for price setting, targeted deals, and advertisements. These practices could further disadvantage small businesses that lack the resources to compete. Ultimately, this bill's prohibition of surveillance pricing seeks to ensure fairness and transparency in competition and pricing.

4) **Concerns with the bill in print.** Price discrimination itself is neither illegal nor is it necessarily harmful for consumers. Surveillance pricing is a form of first-degree price discrimination, in which prices are based on the willingness of the consumer to pay, meaning some consumers pay more or less for the same good or service. Public perception of this practice is largely negative. When consumers were asked if they felt this was a fair practice in 2018, only 8% of respondents responded positively.[15] In contrast, second-degree price discrimination, the practice of offering discounts based on bulk purchases or loyalty programs, or third-degree price discrimination, the practice of offering discounts based on unique demographics such as veterans, students, and retired people, are much more popular. Loyalty programs often offer personalized coupons for products a consumer purchases frequently, necessitating some use and retention of personally identifiable information about a consumer to offer such coupons. Similarly, discount programs targeting specific demographic groups also require consumers to provide personally identifiable information to receive discounts. Both second- and third-degree price discrimination appear to give advantages to consumers.

In opposition, the American Advertising Federation, on behalf of the advertising industry, argues that AB 446 fails to recognize that not all pricing discrimination is bad:

> AB 446 fails to acknowledge the value of these everyday occurrences to consumers and does not draw a distinction between discriminatory practices and personalized pricing strategies that enhance consumer experiences. For example, when a business uses personal data such as IP addresses or browsing activity to infer consumer preferences and offers a 15% discount pop-up during the consumer's visit to the brand's website, this is a legitimate and consumer-friendly use of data. This interaction would be illegal if AB 446 becomes law. Tailored discounts offered to specific consumers at the right time and in the right place reflect a business's ability to understand its customer base and helps drive economic activity. By outlawing such practices, AB 446 would deprive consumers of personalized deals and discounts they value.
>
> […]
>
> AB 446 would undermine loyalty programs and other incentives that many Californians rely on for savings and convenience. Grocery store loyalty programs and associated mobile apps, which use shopper data to offer tailored deals, coupons and other savings, would no longer be allowed to provide the same benefits to consumers in California if AB 446 becomes law. In these times of economic uncertainty, families who depend on these types of programs for

---

[15] Organisation for Economic Co-operation and Development "Personalised Pricing in the Digital Era" (Mar. 10, 2025), https://web-archive.oecd.org/temp/2022-02-22/494784-personalised-pricing-in-the-digital-era.htm.

> budgeting would be negatively impacted by such a dramatic change in loyalty program practices. Similarly, whole industries, such as the automobile industry, would enter a new era where extremely popular car buyback programs could face restrictions. For instance, dealerships would no longer be able to use information known about a vehicle's age and owner to offer a buyback deal, beneficial to both the consumer and the business. AB 446 would reduce the ability of businesses to interact meaningfully with their customers, curbing personalization, stifling options for consumer engagement, and ultimately harming families across California.

Recognizing these concerns, the author has agreed to amend the bill to allow consumers to provide informed consent for businesses to collect and use covered information solely for the purpose of receiving discounts on goods and services.

Another form of price discrimination that must be considered is pricing based on differences in business costs. For example, a plumber performing the same job at two different homes may charge different prices due to accessibility, one home may be in the plumber's neighborhood, while the other is on a remote hill, requiring additional travel time and expenses. As industry opponents state: "Because AB 446 lists 'residence' among its broad list of protected areas, it would appear that setting a price differently for customers who are harder to reach (for example, in a remote and hard-to-reach area) would qualify as 'surveillance pricing.'" Since business costs often require the use of personally identifiable information to set prices, the author has agreed to amend the bill to exempt personalized prices based solely on the cost of providing the good or service to the consumer.

Insurers use personal information to set prices. Finally, opponents note that insurers would likely fall under the umbrella of surveillance pricing, as they use personally identifiable information in their risk-based assessment to set insurance rates. The author has agreed to amend the bill to exclude insurers.

Definition of personally identifiable information. Industry opponents state:

> **AB 446** creates ambiguity around what is covered by the CCPA's term of "personal information" by both *relying on that definition* and *ignoring what is covered under it.* In Proposed Section 7200 (a)(4), **AB 446** identifies the types of data that will be unusable in pricing with a list of categories of data. Among that list is "Personally identifiable information," which is defined by reference to the CCPA's similar term, and includes basically *any consumer information*. Despite this broad term already encompassing virtually *all consumer data*, **AB 446** also lists a number of items that are *already implicitly included* in this definition as separate types of data. In other words: **AB 446** suggests that "actions, habits, …web browsing history, purchase history … [and] consumer behaviors" need to be listed separately because they are not already included by the CCPA's definition of "personal information" … when, in fact, they are already included.

The definition of personally identifiable information covers all activities prescribed in "Electronic surveillance technology" and the author has agreed to amend the bill to address this redundancy.

CalChamber also argues that the inclusion of deidentified or aggregated consumer information in personal information is inherently not personal information. As defined in the CCPA,

"deidentified consumer information" is defined to mean information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer. "Aggregate consumer information" is the information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. However, as the Victorian Information Commissioner in Australia argues, even though aggregate consumer information cannot be used to identify a consumer, it can be used to make general assumptions about a consumer's characteristics:

> In the commercial sphere, for example, if an individual is classified into a group that is considered affluent, a business can potentially charge more for the same service in the knowledge that prospective customer is likely to be able to pay. The classification need not be 100% accurate, it only needs to be right a sufficient number of times to result in increased profits. Coarse location information can be derived from the user's IP address. Even though not personally identifiable on its own, it is sufficient to allow classification of the customer, and for them to be treated differently, potentially to their detriment.[16]

Industry opponents' argument regarding deidentified information has merit, as that information cannot be used to make any assumptions about a consumer. However, aggregate consumer information can be used to set different prices based on general assumptions about groups of people, as discussed above. Therefore, the author has agreed to amend the bill to remove deidentified information and clarify that aggregated consumer information is not personally identifiable information, but continues to be captured under the bill's definition of "surveillance pricing".

Accuracy of findings and declarations. CalChamber raises issues with the breadth and extent of the findings and declarations of this bill, stating that "these allegations appear either incorrect or out-dated." The author has agreed to amend the bill to remove the findings and declarations.

5) **Amendments.** As set forth above, the author has agreed to remove the findings and declarations and to amend the bill to allow for beneficial pricing schemes such as loyalty programs, clarify the definitions and scope of the bill, exclude insurers, and make other clean-up changes. In its entirety, the bill will read as follows:

> **7200.** For purposes of this part, the following definitions apply:
>
> ***(1)*** (a) "Electronic surveillance technology" means a technological method or system of surveillance ~~used to observe, monitor, or collect information related to a person and includes any of the following information about the person:~~ ***used to gather covered information.***
>
> (b) "Person" means a natural person or an entity, including, but not limited to, a corporation, partnership, association, trust, limited liability company, cooperative, or other organization.
>
> (c) "Personally identifiable information" shall have the same meaning as "personal information" as defined in paragraph (1) of subdivision (v) of Section 1798.140 of the Civil

[16] Office of the Victorian Information Commissioner, "The Limitations of De-Identification – Protecting Unit-Record Level Personal Information", (Mar. 13, 2025), https://ovic.vic.gov.au/privacy/resources-for-organisations/the-limitations-of-de-identification-protecting-unit-record-level-personal-information/.

Code and any regulations promulgated thereunder. ~~Notwithstanding paragraph (1) of subdivision (v) of Section 1798.140 of the Civil Code, "personally identifiable information" includes deidentified or aggregated consumer information.~~

(d)"Aggregate consumer information" means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device.

(e) "Covered information" means either personally identifiable information or aggregate consumer information.

(f) "Surveillance pricing" means ~~when a person sets a price offered to a consumer based, in whole or in part, upon personally identifiable information gathered through an electronic surveillance technology, including electronic shelving labels.~~ ***using covered information gathered through electronic surveillance technology to set the price of a commercial good or service for a consumer that differs from the standard price.***

(g) "Standard price" means the price of a good or service that is set for all consumers that is not based upon covered information.

7202. ~~It shall be unlawful for a person to engage in surveillance pricing.~~ ***(a) Except as provided in (b), a person shall not engage in surveillance pricing.***

(b) A person may engage in surveillance pricing if any of the following apply:

(1) The difference from the standard price charged to a consumer is based solely on the cost to the person of providing the good or service to that consumer.

(2) The difference from the standard price is a discount offered to all consumers on equal terms in a manner consistent with applicable anti-discrimination laws. If the person gathers covered information in connection with the provision of this discount, the person shall ensure both of the following:

> ***(A) That the consumer receives a clear and conspicuous written notice describing in readily ascertainable terms the specific intended purposes for which the person will use the information before the person uses the information for any such purpose.***
>
> ***(B) That the consumer provides written affirmative consent for any purpose described in paragraph (1) before their personally identifiable information is used for that purpose.***

(3) The person operates as an insurer complying with Section 791.02 of the Insurance Code.

7204. (a) In addition to any other remedy at law, a person that violates this part shall be liable for a civil penalty for each violation not to exceed the jurisdiction of small claims court for individuals, where each violation means each item of tangible property or each use of a service sold in violation of Section 7202.

(b) A person that intentionally violates this part shall be liable for a civil penalty no greater than three times the amount of the penalty assessed pursuant to subdivision (a) and shall disgorge all revenues earned from the violation.

(c) A prevailing party in an action brought pursuant to this part shall be awarded reasonable attorneys' fees and costs.

7208. Any waiver of this part is against public policy and is void and unenforceable.

SEC. 3. The Legislature finds and declares that this act furthers the purposes and intent of the California Privacy Rights Act of 2020.

ARGUMENTS IN SUPPORT: Consumer Watchdog, a co-sponsor of this bill, writes:

> Unfortunately, the FTC has appeared to shelve its investigation into surveillance pricing, which makes the work of California legislators that much more important. AB 446 aims to address these concerns by prohibiting businesses from setting prices based on personally identifiable information gathered through electronic surveillance. The bill seeks to bar companies from using race, religion, residence, sexuality, political interests, web browsing and purchase history, financial circumstances, and consumer behaviors in setting prices. The bill also outlines civil penalties for violations, ensuring that consumers are protected from such exploitative practices.
>
> As you've [Assemblymember Ward] said, "At a time when prices for basic necessities are rising across the board, it is more critical than ever to ensure that people are not being unfairly charged higher prices due to their actual or perceived characteristics."
>
> AB 446 demonstrates a commitment to consumer rights and privacy, ensuring that all Californians are treated fairly in the marketplace. One product, one price.

The UCFW Western States Council, a co-sponsor of this bill, writes:

> Surveillance pricing also pre-ordains that today's Big Tech hegemons will be able inevitably to extend their dominance even further over every aspect of commerce. Under a surveillance pricing-dominant regime, the few companies with the most data, the world's most powerful computers, and the most state-of-the-art AI will have a permanent and ever-increasing advantage over their homely, better mousetrap-manufacturing competitors.
>
> The cost for an innovator to enter a surveillance-dominated market will just be too high. If an innovator does somehow gain a market share, the company's investors will prefer selling to the hegemons over trying to compete with them; already standard operating procedure for today's internet and pharmaceutical start-ups. This may now be common but it is not how competitively functioning markets are supposed to work.

ARGUMENTS IN OPPOSITION: In opposition to the bill, a coalition of trade groups, including California Chamber of Commerce, states:

> The California Consumer Privacy Act ("CCPA") is the definitive statute related to consumers' privacy and their personal data – whether that data is collected online, in brick-

and-mortar stores, by technological means, on paper, or by powers of observation. In other words, it is a broad, technology-neutral, industry-neutral, and comprehensive consumer data protection law, which was also voter-approved via Proposition 24 in 2020. Substantively, the CCPA governs how a company may collect data related to a customer's behavior (buying certain products, for example) and utilize that data. The CCPA also already addresses permissible and impermissible business uses of consumer data for activities such as targeted advertising, loyalty and rewards programs, and the like. In fact, the CCPA places limits on the sharing of customers' data, allowing customers to opt-out of allowing a business to share such data.

AB 446 also seeks to control how businesses collect and use a consumer's data—an aim that squarely falls under the jurisdiction of the voter-approved CCPA. In doing so, AB 446 completely ignores the CCPA's voter-endorsed provisions and its careful balancing of the complex policy issues around online marketplaces … and simply bans the use of such data in pricing.

REGISTERED SUPPORT / OPPOSITION:

Support

Consumer Watchdog (Co-Sponsor)
Ufcw - Western States Council (Co-Sponsor)
American Federation of Musicians, Local 7
Athena Coalition
California Federation of Labor Unions, Afl-cio
California Nurses Association
California School Employees Association
California State Legislative Board of Smart – Transportation Division (smart – Td)
Cft- a Union of Educators & Classified Professionals, Aft, Afl-cio
Consumer Attorneys of California
Consumer Federation of America
Consumer Federation of California
Economic Security California Action
Electronic Privacy Information Center (EPIC)
Oakland Privacy
Privacy Rights Clearinghouse
Techequity Action
Udw/afscme Local 3930
Western Center on Law & Poverty

Opposition

American Advertising Federation (AAF)
American Association of Advertising Agencies (4A's)
American Property Casualty Insurance Association
Associated Equipment Distributors
Association of National Advertisers
Calbroadband
California Attractions and Parks Association

California Chamber of Commerce
California Grocers Association
California Hotel & Lodging Association
California New Car Dealers Association
California Retailers Association
California Travel Association
Digital Advertising Alliance
Interactive Advertising Bureau
National Association of Mutual Insurance Companies
National Federation of Independent Business
Personal Insurance Federation of California
Software Information Industry Association
Technet
The Travel Technology Association

Analysis Prepared by: John Bennett / P. & C.P. / (916) 319-2200